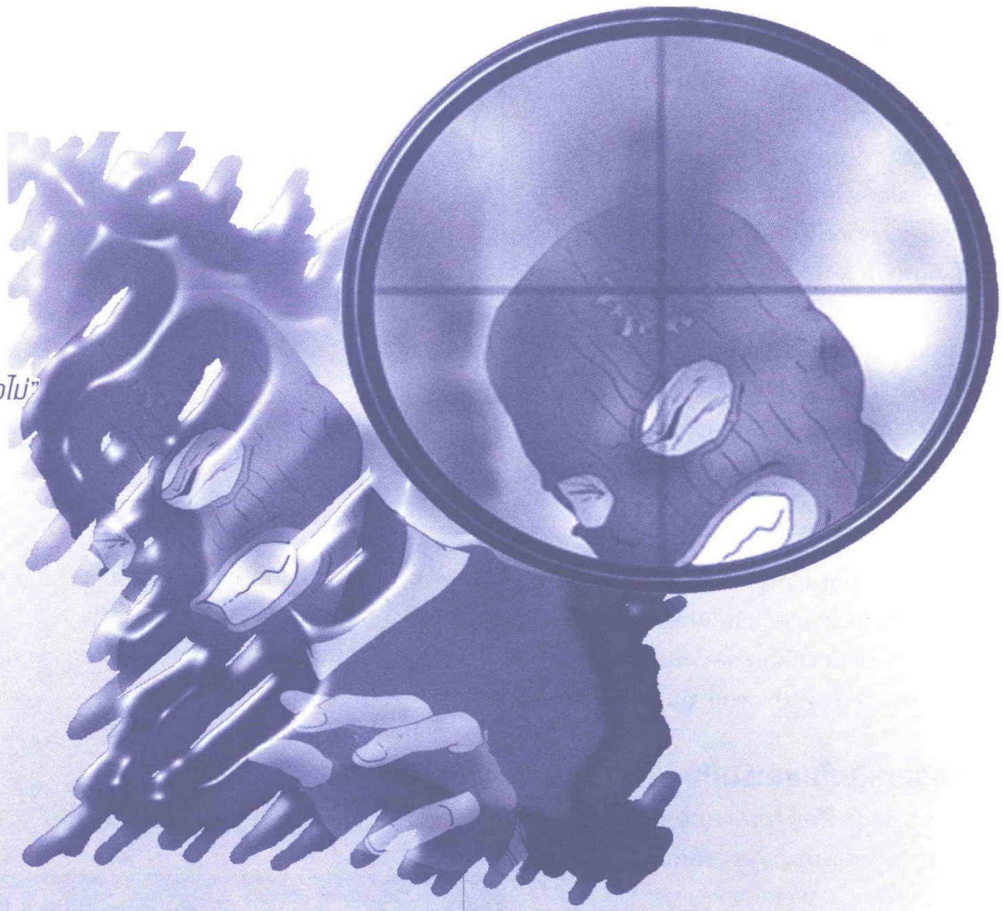
■ปิยะ สมบุญสำราญ
piya@egat.or.th

สมรภูมิเดือด เมื่อแฮกเกอร์แผลงฤทธิ์

"สำรวจเครือข่ายของท่านหรือยัง ว่าเปิดช่องทางไว้ให้บุกรุกบ้างหรือไม่"



เรื่องราวของไสยศาสตร์กับวิทยาศาสตร์บางครั้งใกล้เคียงกันแทบไม่น่าเชื่อ การรักษาความปลอดภัยสำหรับระบบเครือข่ายก็เป็นอีกตัวอย่างหนึ่งที่เข้าข่ายนี้ ผู้บุกรุกระบบเครือข่ายหรือแฮกเกอร์นั้นไม่ได้บุกรุกระบบเครือข่ายด้วยตัวตนจริง ๆ หรือกายหยาบ แต่เป็นการบุกรุกด้วยการใช้กายเสมือนหรือกายทิพย์เดินทางมายังระบบเครือข่าย คล้ายกับการถอดจิตเข้ามา พอเปรียบเทียบอย่างนี้ฟังดูแล้วน่ากลัวเหมือนกับว่ากำลังถูกบุกรุกด้วยสิ่งที่ไม่มีตัวตนและมองไม่เห็น และความรู้สึกของผู้ถูกบุกรุกก็เป็นเช่นนั้นจริง ๆ บางครั้งรู้ว่าถูกบุกรุกแน่ ๆ แต่ก็หาสาเหตุไม่ได้ บางครั้งมีคนเขามาในระบบแต่ก็หาที่มาที่ไปไม่ได้ และในบางครั้งถูกบุกรุกไปแล้วยังไม่ทราบเลยว่าถูกบุกรุก เมื่อเป็นเช่นนี้เวลาเกิดเหตุการณ์แปลก ๆ ขึ้นในระบบที่ไม่สามารถอธิบายได้ ก็จะเหมารวมว่าถูกบุกรุกระบบไปเลย บางครั้งเป็นอันรู้กันเลยว่าถ้าผู้ดูแลระบบถูกผีหลอกแล้วละก็จะหมายถึงว่าระบบเครือข่ายกำลังถูกบุกรุกจากแฮกเกอร์

ผู้ที่เดือดร้อนกับการบุกรุกระบบเครือข่ายเห็นจะไม่พ้นผู้ดูแลระบบเครือข่าย ซึ่งตามปรกติก็จะมีงานล้นมืออยู่แล้ว ยังต้องแบ่งเวลามาให้กับระบบรักษาความปลอดภัยเพิ่มขึ้นอีก และงานนี้ไม่ใช่งานที่สามารถปล่อยปละละเลยได้ ต้องทำด้วยความละเอียดรอบคอบ และต้องใช้เวลามาก ทำให้มากินเวลาของงานประจำที่ทำอยู่ซึ่งจะทำให้งานประจำไม่ก้าวหน้าเท่าที่ควร

อย่างไรก็ตามการถูกบุกรุกระบบนั้นไม่สามารถหลีกเลี่ยงได้ แม้กระทั่งเครือข่ายที่ทำหน้าที่ดูแลเกี่ยวกับระบบรักษาความปลอดภัยโดยตรงเองก็ยังถูกบุกรุก แต่การบุกรุกนั้นจะเป็นในรูปแบบใดจะทำอันตรายต่อระบบเครือข่ายหรือไม่ และจะมีหนทางใดบ้างที่สามารถทำให้ระบบเครือข่ายของเราอยู่รอดปลอดภัยจากการบุกรุก วันนี้เราจะมาพูดถึงเรื่องเหล่านี้กันครับ ผู้เขียนจะขอยกตัวอย่างประสบการณ์อันโชกโชนมาเล่าให้ฟังนะครับ แต่เป็นประสบการณ์ที่แตกต่างออกไปคือไม่ใช่ประสบการณ์ในฐานะของผู้บุกรุก แฮกเกอร์ หรือผู้กระทำ แต่จะมาเล่าให้ฟังในฐานะผู้ที่ถูกบุกรุกหรือผู้ที่ถูกกระทำแทน โดยจะเล่าให้ฟังถึงในแง่มุมต่อไปนี้

- ภาพรวมของการรักษาความปลอดภัยสำหรับระบบเครือข่าย
- แค่ไหนถึงเรียกว่าถูกบุกรุก
- ตัวอย่างการออกแบบระบบรักษาความปลอดภัย
- ทำไมระบบเครือข่ายจึงถูกบุกรุกได้
- รู้รั่วของระบบเครือข่ายไม่ยากที่ตรวจพบและแก้ไข
- จะใครเป็นคนผิดในเรื่องของระบบรักษาความปลอดภัย

ภาพรวมของการรักษาความปลอดภัยสำหรับระบบเครือข่าย

ระบบรักษาความปลอดภัยบนเครือข่ายจะคล้ายคลึงกับระบบรักษาความปลอดภัยของสำนักงานหรือที่อยู่อาศัยครับ ซึ่งจะมีพนักงานรักษาความปลอดภัย ประตูทางเข้า ห้องรับแขก ห้องทำงาน ห้องนอน ฯลฯ การเข้าถึงส่วนต่างๆ ของสำนักงานก็ต้องมีขั้นตอนในการผ่านเช่นเดียวกับการเข้าถึงข้อมูลในระบบเครือข่ายก็ต้องมีขั้นตอนในการเข้าถึงเช่นกัน ดังตัวอย่างในรูปที่ 1 เป็นตัวอย่างระบบรักษาความปลอดภัยของสำนักงาน

เราจะสมมุติเหตุการณ์ว่ามีบุคลลภายนอกต้องการติดต่อกับสำนักงานแห่งหนึ่งแล้วลองติดตามดูว่าจะต้องผ่านเส้นทางใดและผ่านการตรวจสอบจากระบบรักษาความปลอดภัยอย่างไรบ้าง

เมื่อจะมีผู้คนเข้ามาติดต่องานก็จะต้องผ่านจุดต่าง ๆ ของสำนักงานดังนี้

1. ผ่านประตูรั้วของสำนักงาน
2. เดินผ่านทางเดินจากรั้วมายังประตูหน้าของสำนักงาน
3. เปิดประตูหน้า
4. เดินผ่านประตูหน้ามายังห้องรับแขกเพื่อติดต่อประชาสัมพันธ์
5. เดินจากห้องรับแขกไปยังประตูห้องทำงาน
6. เปิดประตูห้องทำงานเพื่อผ่านเข้าไปสู่ส่วนอื่นๆ ภายในสำนักงาน

คราวนี้เรามาลองเปรียบเทียบกับระบบเครือข่ายได้ดังนี้

คำอธิบายรูป

ไฟล์วอร์

ไฟล์วอร์หรือประตูกันไฟในระบบเครือข่ายนี้เป็นอุปกรณ์สำหรับรักษาความปลอดภัยจากผู้บุกรุกระบบเครือข่าย เปรียบเหมือนพนักงานรักษาความปลอดภัยของระบบเครือข่าย ที่ทำหน้าที่ตรวจสอบข้อมูลที่วิ่งผ่านเข้าออกและคอยตรวจสอบสิทธิ์ของผู้ผ่านเข้าออกระบบเครือข่ายว่าสามารถเข้าถึงข้อมูลใดได้บ้าง โดยในระบบตัวอย่างจะติดตั้งไฟล์วอร์จำนวน 3 ตัวแต่ละตัวจะทำหน้าที่ดังนี้

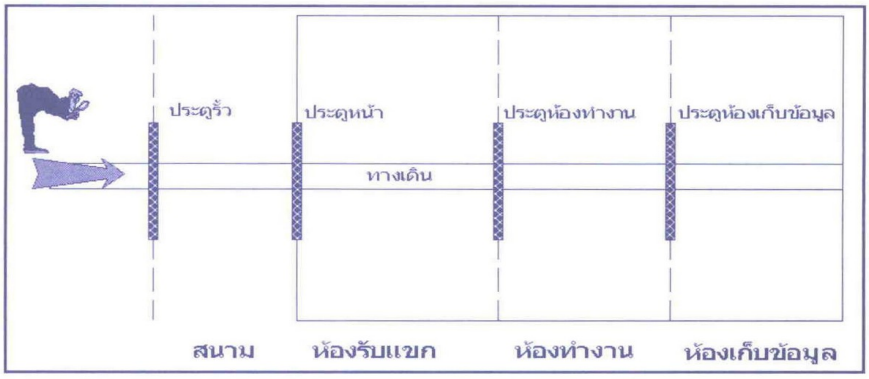
ไฟล์วอร์ตัวที่ 1 ทำหน้าที่รักษาความปลอดภัยจากเครือข่ายภายนอก

ไฟล์วอร์ตัวที่ 2 ทำหน้าที่รักษาความปลอดภัยจากเครือข่ายภายใน

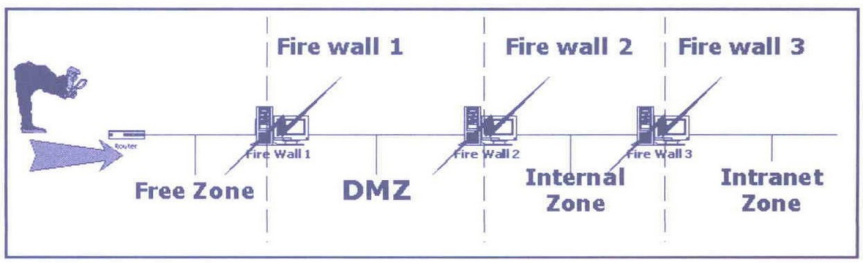
ไฟล์วอร์ตัวที่ 3 ทำหน้าที่รักษาความปลอดภัยแก่ข้อมูลพิเศษ

เราเตอร์

เป็นอุปกรณ์เชื่อมโยงข้อมูลระยะไกล เนื่องจากระบบแลนด์ตามปรกติจะต่อได้ระยะไม่เกินร้อยเมตร หากระยะทางไกลกว่านี้ เช่นการเชื่อมโยงข้ามตึก การเชื่อมโยงระหว่างสาขาของสำนักงานต่าง ๆ การเชื่อมโยงระหว่างสำนักงานและศูนย์บริการอินเทอร์เน็ต ฯลฯ ก็ต้องใช้เราเตอร์ช่วยเชื่อมต่อ



รูปที่ 1 ตัวอย่างระบบรักษาความปลอดภัยของสำนักงาน



รูปที่ 2 ตัวอย่างระบบรักษาความปลอดภัยของระบบเครือข่าย

เมื่อมีผู้คนเข้ามาติดต่อขอข้อมูลในระบบเครือข่ายจะต้องผ่านขั้นตอนดังนี้

1. ผ่านเข้าเราเตอร์ของระบบเครือข่าย
2. ผ่านเขต Free Zone จากเราเตอร์มายังไฟล์วอร์
3. ข้อมูลส่งผ่านไฟล์วอร์
4. ผ่านเข้ามายังส่วนของ DMZ
5. ผ่านเขต DMZ ไปยัง Web Server
6. ขออนุญาติเรียกดูข้อมูลอื่น ๆ ภายในจากไฟล์เวอร์ตัวที่สอง

สำหรับความหมายของ Free Zone DMZ จะไม่กล่าวถึงรายละเอียดในหัวข้อถัดไป ตอนนี้เพื่อให้เห็นภาพรวมของระบบรักษาความปลอดภัชัดเจนขึ้นให้ท่านผู้อ่านดูการข้อเปรียบเทียบดังตารางที่ 1

ตัวอย่างการแบ่งส่วนระบบรักษาความปลอดภัย

จากตัวอย่างของระบบรักษาความปลอดภัยในระบบเครือข่าย ตามรูปที่ 2 จะมีการแบ่งส่วนของระบบรักษาความปลอดภัยของเครือข่ายออกเป็น 4 ส่วน ดังนี้

- Free Zone
- DMZ Zone
- Internal Server
- Intranet Zone

Free Zone

เปรียบได้กับเครือข่ายหน้าบ้านหรือสนามหน้าบ้าน เป็นบริเวณที่ยังไม่ผ่านระบบไฟล์วอร์ จะอยู่หลังเราเตอร์และอยู่หน้าไฟล์วอร์ตัวแรก บริเวณนี้จะไม่อยู่ภายใต้ระบบรักษาความปลอดภัยใด ๆ มักจะไว้ติดตั้งระบบทดสอบที่ต้องการทดสอบโดยไม่ผ่านไฟล์วอร์ หรือติดตั้งระบบตรวจสอบข้อมูลเข้าออก

ตามปรกติใน Free Zone นี้จะไม่ติดตั้งเซิร์ฟเวอร์สำหรับใช้งานจริงเนื่องจากจะถูกบุกรุกระบบได้ง่าย

DMZ Zone

DMZ (DeMilitarize Zone) เปรียบเหมือนกับห้องรับแขกภายในสำนักงานซึ่งมีจะหน่วยงานประชาสัมพันธ์คอยติดต่อกับผู้ที่มาติดต่อ เป็นเขตที่อยู่หลังไฟล์วอร์ตัวแรก และอนุญาติให้บุคคลทั่วไปจากเครือข่ายภายนอกสามารถเรียกดูข้อมูลในเขตนี้ได้ โดยอยู่ภายใต้ความควบคุมของไฟล์วอร์ เครื่องที่ให้บริการที่ตั้งอยู่ในเขตนี้ได้แก่เครื่อง WWW, Email, FTP

Internal Zone

เป็นเขตที่ติดตั้งเครื่องให้บริการของสำนักงาน เป็นเขตที่อยู่หลังไฟล์วอร์ตัวที่สองไม่อนุญาติให้บุคคลภายนอกเรียกดูข้อมูลแต่จะอนุญาติให้บุคคลภายในสามารถเรียกดูข้อมูลได้ภายใต้ระบบรักษาความปลอดภัยโดยอยู่ภายใต้ความควบคุมของไฟล์วอร์ตัวที่ 2 และไฟล์วอร์ตัวที่ 3

Intranet Zone

เป็นส่วนของระบบเครือข่ายภายในสำนักงานหรือภายในองค์กร สามารถติดต่อกับส่วนอื่น ๆ ได้โดยผ่านระบบรักษาความปลอดภัยตามลำดับขั้น แต่จะไม่อนุญาติให้บุคคลจากเครือข่ายภายนอกเรียกดูข้อมูลในส่วนนี้ และไม่สามารถติดต่อกับระบบเครือข่ายภายได้โดยตรง

เครื่องคอมพิวเตอร์ใน Internet Zone นี้สามารถเรียกดูข้อมูลภายนอกได้แต่ต้องภายระบบรักษาความปลอดภัยต่าง ๆ เช่น Proxy, NAT, Sock ฯลฯ

รายละเอียดในแต่ละส่วนและวิธีการออกแบบนั้นคงต้องเอาไว้หาโอกาสคุยกันเป็นตอนพิเศษนะครับ ตอนนี้เราดูกันที่ภาพรวมก่อน เมื่อมีระบบรักษาความปลอดภัยแล้วสิ่งที่คู่กันก็คือการบุกรุกระบบเครือข่ายครับ แล้วแค่ไหนละถึงจะเรียกว่าถูกบุกรุก....

แค่ไหนถึงจะเรียกว่าถูกบุกรุก

คำว่าบุกรุกนี้ก็มีความหมายที่สับสนเหมือนกันอย่างเวลาเราเดินผ่านบ้านใครแล้วแอบมองเฉย ๆ โดยไม่ได้ทำอะไรแล้วถือว่าเป็นการบุกรุกหรือเปล่า แล้วถ้าเจ้าของบ้านเขาลืมเปิดประตูทิ้งไว้แล้วเราเดินเข้าไปถือว่าเป็นการบุกรุกหรือเปล่า ดังนั้นก่อนอื่นต้องนิยามความหมายของคำว่าบุกรุกก่อน ผู้เขียนจะแบ่งระดับของการบุกรุกออกเป็น 2 ระดับดังนี้ครับ

- **บุกรุกด้วยสายตา**
- **บุกรุกด้วยกำลัง**

การบุกรุกเครือข่ายทั้งสองระดับนี้เป็นความพยายามที่จะเข้าถึงข้อมูลในเครือข่ายโดยที่เจ้าของไม่ต้องการให้ดูข้อมูลหรือเป็นการเข้าดูโดยไม่ได้รับอนุญาติ ไม่ว่าจะทำสำเร็จหรือไม่สำเร็จก็ตามก็ถือว่าเป็นการบุกรุกระบบแล้ว แต่ถ้าเป็นการเข้าถึงขอมูล

ขั้นตอน	ขั้นตอนของระบบรักษาความปลอดภัย		ผู้ทำหน้าที่/อุปกรณ์ป้องกัน	
	สำนักงานฯ	ระบบเครือข่ายฯ	สำนักงาน	ระบบเครือข่าย
1.	ผ่านประตูรั้วของสำนักงาน	ผ่านเข้าเราเตอร์ของระบบเครือข่าย	ยาม, ประตูรั้ว	เราเตอร์
2	เดินผ่านทางเดินจากรั้วมายังประตูหน้าของสำนักงาน	ผ่านเขต Free Zone จากเราเตอร์มายังไฟล์วอร์	ไม่มี	ไม่มี
3	เปิดประตูหน้า	ข้อมูลส่งผ่านไฟล์วอร์	ยาม, ประตูหน้า	ไฟล์วอร์ตัวแรก
4	เดินผ่านประตูหน้ามายังห้องรับแขก	ผ่านเข้ามายังส่วนของ DMZ	ไม่มี	ไม่มี
5	เดินจากห้องรับแขกไปยังประตูห้องทำงาน	ผ่านเขต DMZ ไปยัง Web Server	ยาม,ประตูห้องทำงาน	ไฟล์วอร์ตัวที่สอง
6	เปิดประตูห้องทำงานเพื่อผ่านเข้าไปสู่ส่วนอื่นๆ ภายในสำนักงาน	ขออนุญาติเรียกดูข้อมูลอื่นๆ ภายในจากไฟล์เวอร์ตัวที่สอง	ประตู	ไฟล์วอร์ตัวที่สาม

ตารางที่ 1 แสดงการเปรียบเทียบระบบรักษาความปลอดภัยของสำนักงานและระบบเครือข่าย

ที่ได้รับอนุญาติแล้วไม่ว่าจะเป็นข้อมูลที่ลับเพียงใดก็ไม่ถือว่าเป็นการบุกรุก สำหรับการบุกรุกในแต่ละระดับแตกต่างกันดังนี้

บุกรุกด้วยสายตา

การที่เราเดินผ่านหน้าบ้านใครคนหนึ่งแล้วแอบมองเข้าไปในบ้าน ผู้เขียนถือว่าเป็นการบุกรุกอย่างหนึ่งครับแต่เป็นการบุกรุกด้วยสายตา ถึงไม่ก่อให้เกิดความเสียหายใด ๆ ต่อสิ่งของภายในบ้าน หรือไม่ได้นำสิ่งของใด ๆ ออกไป แต่การเราที่แอบมองบ้านคนอื่นนี้เราอาจจะเห็นบางสิ่งบางอย่างที่เจ้าของ บ้านเขาไม่ต้องการให้ใครเห็นได้ เช่นห้องรับแขกที่ยังไม่ได้จัด ทีวีที่ยังไม่ได้เซ็ด อาจจะมองลึกเข้าไปถึงห้องนอน ห้องน้ำได้ ถ้าเจ้าของปิดประตูไม่สนิท

การบุกรุกด้วยสายตาในระบบเครือข่ายนั้นสามารถทำได้โดยง่าย เนื่องจากระบบเครือข่ายโดยส่วนใหญ่จะไม่มีการป้องกันในส่วนนี้ หรือว่าไม่มีความจำเป็นที่จะป้องกัน เช่น

- หมายเลขไอพีแอดเดรสของเครื่อง
- จำนวนเครื่องเซิร์ฟเวอร์ในระบบ
- สถานะของเครื่อง
- จำนวนผู้ใช้งานที่กำลังใช้งานอยู่
- ตรวจสอบชื่อเจ้าของโดเมน
- ตรวจสอบการให้บริการต่างๆ

ข้อมูลเหล่านี้ผู้ที่อยู่นอกเครือข่ายสามารถตรวจสอบหรือแอบดูได้ เพื่อให้การติดต่อระหว่างเครือข่ายทำได้สะดวกขึ้น และผู้ดูแลระบบบางท่านก็ไม่ถือว่าการตรวจสอบข้อมูลเหล่านี้เป็นการบุกรุก แต่ข้อมูลเหล่านี้ก็จะเป็นข้อมูลเบื้องต้นสำหรับการบุกรุกขั้นรุนแรงต่อไปเช่นกัน ซึ่งถ้าแฮกเกอร์ไม่ทราบข้อมูลเบื้องต้นเหล่านี้ก็จะทำงานได้ลำบากขึ้น ลองดูสักตัวอย่างนะครับ สมมุติว่าเราจะตรวจสอบหรือแอบดูเครื่องข่ายสักเครือข่ายหนึ่งเราจะทำอะไรได้บ้าง

1. ตรวจสอบหมายเลขไอพีของเครือข่ายที่ต้องการ
2. ตรวจสอบสถานะของเครื่องในระบบว่ามีเครื่องใดเปิดอยู่บ้าง
3. ตรวจสอบจำนวนผู้ใช้งานในแต่ละเครื่อง
4. ตรวจสอบโปรแกรมที่ติดตั้งอยู่บนเครื่องให้บริการต่างๆ
5. ตรวจสอบว่าจุดบกพร่องของโปรแกรม
6. ตรวจสอบเส้นทางการส่งข้อมูลไปยังเครือข่ายเป้าหมาย
7. ตรวจสอบรูรั่วของระบบเครือข่าย
8. บุกรุกระบบเครือข่ายตามรูรั่วที่พบ

ขั้นตอนในการบุกรุกขั้นที่ 1-6 เป็นความสามารถพื้นฐานของผู้ดูแลระบบทุกคนอยู่แล้วครับไม่ใช่เรื่องที่ปกปิดหรือเรื่องที่เป็นความลับแต่อย่างไร และเป็นขั้นตอนธรรมดาที่ผู้ดูแลระบบใช้ในการตรวจสอบระบบเครือข่าย สมมุติว่าเรากำลังตรวจสอบระบบเครือข่ายหนึ่งเพื่อทำการบุกรุก ชื่อเครือข่ายคือ www.piya.com เราก็จะเริ่มขั้นตอนดังนี้

ขั้นตอนที่ 1 ตรวจสอบหมายเลขไอพีของเครือข่ายที่ต้องการ

ตรวจสอบหมายเลขไอพีของเครือข่าย www.piya.com โดยใช้คำสั่ง ping (คำสั่งนี้มีทั้งบนวินโดวส์และยูนิกส์)

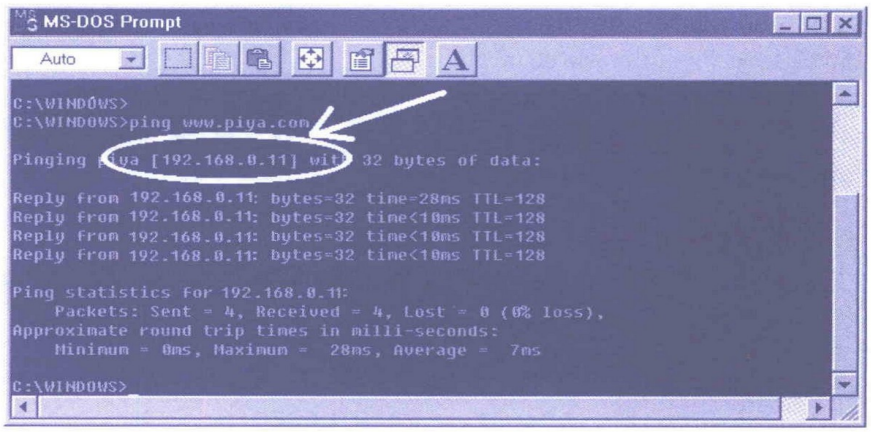
ผลลัพธ์ของคำสั่ง ping จะแสดงหมายเลขไอพีของเครื่อง www.piya.com เป็น 192.168.0.11 (หมายเลขสมมุติ) คราวนี้ก็ใช้ความรู้พื้นฐานของระบบเครือข่ายเรื่อง TCP/IP Network มาประกอบครับ

- หมายเลขไอพีจะประกอบไปด้วยตัวเลขจำนวน 4 ชุด
- ตามปรกติแล้วเครื่องคอมพิวเตอร์ในระบบเดียวกันจะมีหมายเลขไอพีเหมือนกัน 3 ชุด
- แต่ละชุดจะมีค่า 0 ถึง 255
- ไอพีแอดเดรสของเครื่องคอมพิวเตอร์จะอยู่ระหว่าง 1-255

จากข้อมูลเหล่านี้ก็จะทราบว่าไอพีแอดเดรสของเครือข่าย piya.com นี้จะอยู่ในช่วง 192.168.0.1 ถึง 192.168.0.254 ซึ่งเครื่องให้บริการต่าง ๆ ก็จะมีไอพีแอดเดรสอยู่ในช่วงนี้

ขั้นตอนที่ 2 ตรวจสอบสถานะของเครื่องว่ามีเครื่องใดเปิดอยู่บ้าง

พอเราได้หมายเลขไอพีแอดเดรสมาแล้ว ขั้นตอนต่อไปก็คือตรวจสอบว่ามีเครื่องอยู่กี่เครื่องที่เปิดใช้งาน การตรวจสอบนั้นสามารถทำโดยคำสั่ง ping เช่นเดียวกันครับ โดยการใช้คำสั่ง ping ตามด้วยไอพีแอดเดรสที่ต้องการ โดยการไล่ ping ตั้งแต่ไอพีแอดเดรส 192.168.0.1 ถึง 192.168.0.1 ครับ ถ้าไอพีแอดเดรสใดมีการใช้งานอยู่ก็จะตอบรับคำสั่ง ping กลับมาดังรูปที่ 4 แต่ถ้าไม่มีการใช้งานไอพีแอดเดรสผลลัพธ์ของคำสั่ง ping ก็จะเป็นอย่างอื่นดังรูปที่ 5



รูปที่ 3 ใช้คำสั่ง ping ตรวจสอบหาไอพีแอดเดรสของเครื่อง www.piya.com

ลองไล่ใช้คำสั่ง ping ครบทุกไอพีแอดเดรสก็จะทราบว่ามีเครื่องคอมพิวเตอร์เปิดใช้งานอยู่กี่เครื่อง

ขั้นตอนที่ 3 ตรวจสอบจำนวนผู้ใช้งานในแต่ละเครื่อง

หลังจากที่ทราบแล้วว่ามีเครื่องให้บริการที่ไอพีแอดเดรสใดบ้างแล้ว ต่อไปก็คือการตรวจสอบจำนวนผู้ใช้งานในแต่ละเครื่อง ขั้นตอนนี้จะใช้คำสั่ง finger ในระบบปฏิบัติการยูนิกส์ครับ

จากรูปที่ 6 แสดงรายชื่อผู้ใช้งานที่กำลังใช้งานอยู่บนเครื่อง 192.168.0.11 เมื่อเห็นรายชื่อผู้ใช้งานแล้วก็เป็นข้อมูลที่จะทดลองบุกรุกระบบเครือข่ายในระดับที่รุนแรงขึ้น เช่นทดลองเดารหัสผ่านของผู้ใช้งาน

ขั้นตอนที่ 4 ตรวจสอบโปรแกรมที่ติดตั้งอยู่บนเครื่องต่าง ๆ

โปรแกรมที่ให้บริการบนอินเทอร์เน็ตจะมีหมายเลขหรือพอร์ตสำหรับการให้บริการเฉพาะ ถ้าเราต้องการทราบว่ามีโปรแกรมให้บริการอยู่บ้างก็จะใช้วิธีติดต่อไปที่พอร์ต เหล่านั้น โดยใช้คำสั่ง telnet ไปยังพอร์ตที่ให้บริการ เช่นพอร์ต 80 เป็นพอร์ตสำหรับการให้บริการ WWW เราก็ใช้คำสั่งตรวจสอบดังรูปที่ 7

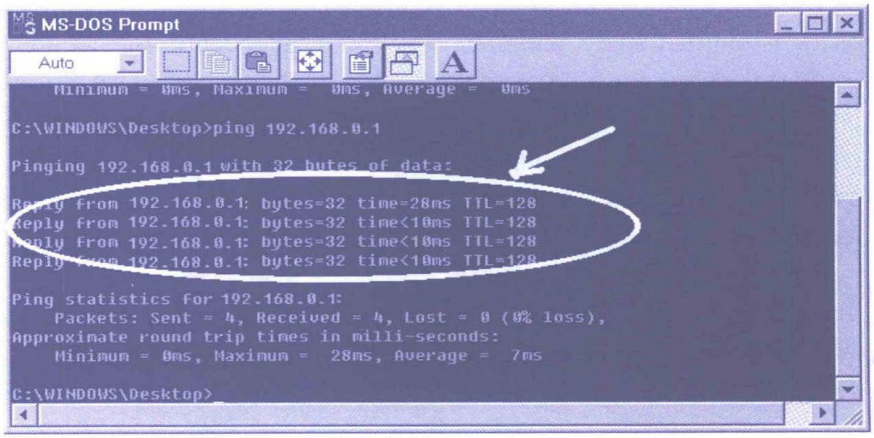
ตามปรกติเมื่อติดต่อเข้าไปยังพอร์ตต่าง ๆ จะมีข้อความแจ้งว่าโปรแกรมที่บริการอยู่ชื่ออะไรเวอร์ชั่นไหน เราก็นำข้อมูลนี้ไปเปรียบเทียบว่าโปรแกรมดังกล่าวมีรูรั่วหรือไม่ จากตัวอย่างในรูปที่ 7 หลังจากใช้ทำสั่ง telnet ติดต่อไปที่พอร์ต 80 แล้วจะเห็นข้อความที่แสดงว่าพอร์ตนี้มีโปรแกรมอะไร รุ่นอะไรทำงานอยู่ จากนี้ก็จะค้นหาว่าโปรแกรม นี้รุ่นนี้มีรูรั่วตรงไหนบ้าง

ขั้นตอนที่ 5 - 7 เป็นการแอบดูที่รุนแรงขึ้นเรายังไม่กล่าวถึงในที่นี้ครับ

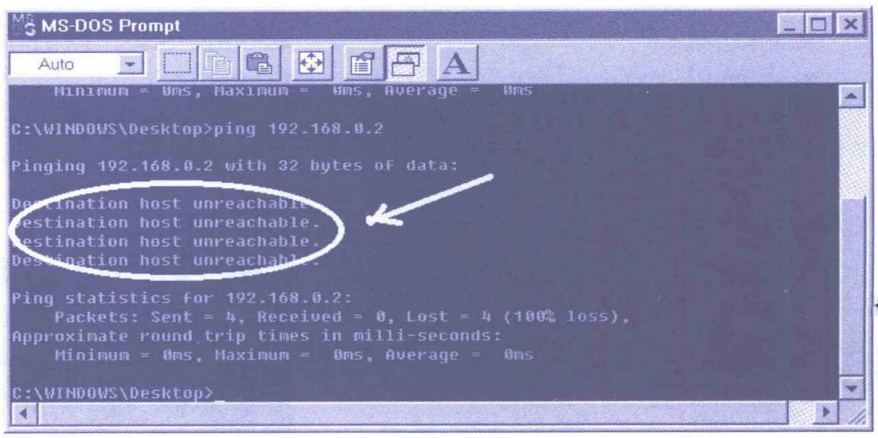
การบุกรุกในลักษณะนี้เหมือนกับการบุกรุกด้วยสายตา ซึ่งบางระบบเครือข่ายอาจจะติดตั้งม่านกันไม่ให้มองเห็นได้ แต่ในการบุกรุกในระดับนี้ยังไม่ถือว่ามีความรุนแรงหรือทำอันตรายต่อระบบเครือข่าย

ขั้นตอนที่ 8 บุกรุกระบบตามรูรั่วที่พบ

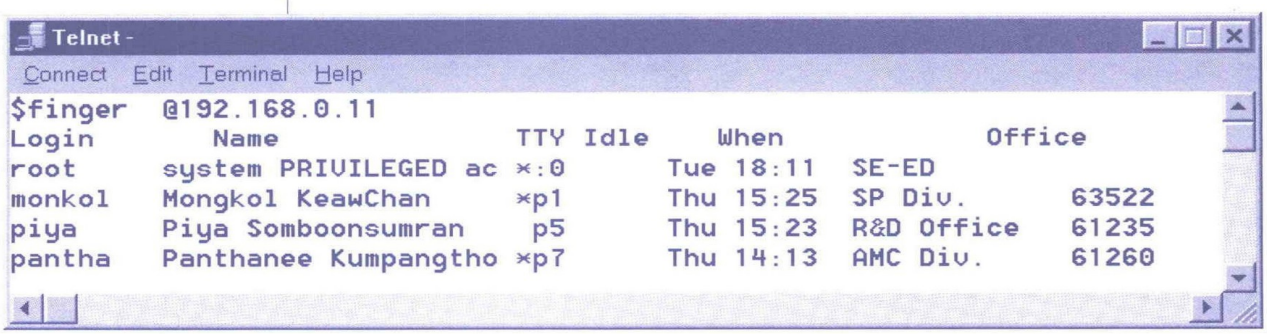
เมื่อทราบข้อมูลเบื้องต้นเรียบร้อยทั้ง 7 ขั้นตอนแล้ว ขั้นตอนต่อไปก็คือการบุกรุกระบบจริงตามรูรั่วที่ตรวจพบ ขั้นตอนนี้ถือว่าเป็นการบุกรุกโดยใช้กำลังและเป็นความตั้งใจที่จะบุกรุกเข้ามาในระบบ ส่วนจะบุกรุกเข้ามาได้หรือไม่นั้นขึ้นอยู่กับว่ารูรั่วต่างๆ นั้นได้รับการแก้ไขแล้วหรือยัง



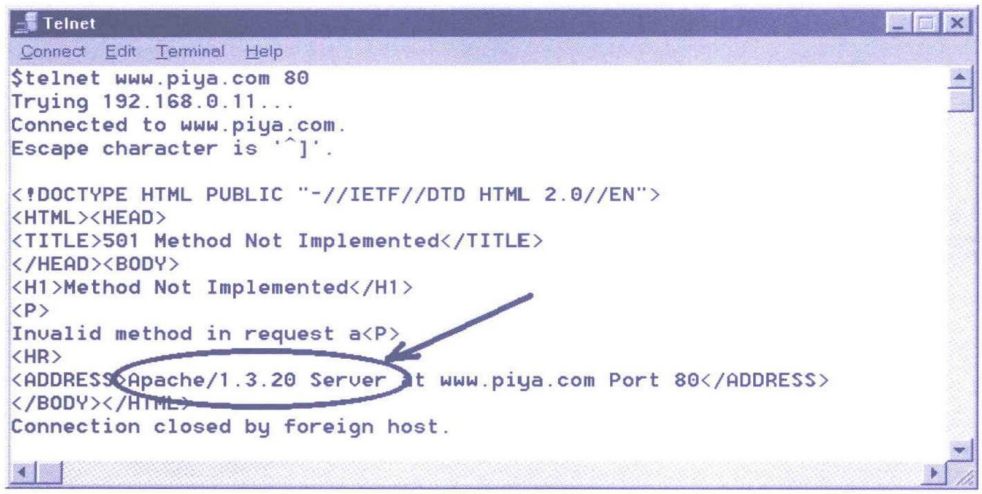
รูปที่ 4 แสดงการตรวจสอบเครื่องไอพีแอดเดรส 192.168.0.1 ซึ่งมีการใช้งานอยู่



รูปที่ 5 แสดงการตรวจสอบ 192.168.0.2 ซึ่งไม่มีการใช้งาน



รูปที่ 6 แสดงการตรวจสอบผู้ใช้งานในเครื่องไอพีแอดเดรส 192.168.0.11



รูปที่ 7 แสดงการตรวจสอบพอร์ต 80 เพื่อดูว่ามีการให้บริการ WWW หรือไม่

การบุกรุกโดยใช้กำลัง

หลังจากที่บุกรุกโดยสายตาโดยการแอบดูบ้านคนอื่นอยู่สักพักหนึ่งแล้วก็จะเริ่มการบุกรุกขั้นต่อไป คราวนี้ไม่เพียงแต่ดูเฉย ๆ แล้วจะเดินเข้ามาในบ้านจริง ๆ ถ้าเจ้าของบ้านเปิดประตูทิ้งไว้ก็อาจจะเดินเข้ามาเฉย ๆ โดยไม่ต้องออกแรงในขณะที่หากเจ้าของบ้านปิดประตูไว้อาจต้องใช้กำลังปีนหรือพังประตูเข้ามา

การบุกรุกโดยใช้กำลังกับระบบเครือข่ายนี้คือการล่วงล้ำเข้ามาในระบบจริง ๆ ไม่ใช่การแอบดูข้อมูลเหมือนกรณีที่แล้วในขั้นตอนที่ 8 ของตัวอย่างที่ยกมา คือการบุกรุกเข้ามาทางรูรั่วของระบบเครือข่าย การกระทำลักษณะนี้ ผู้ดูแลระบบทุกท่านถือว่าเป็นการบุกรุกโดยตั้งใจและถือว่าเป็นการกระทำที่ทำโดยไม่ได้รับอนุญาตและเป็นความผิดโดยเจตนา จะอ้างว่าก็ระบบมีรูรั่วเองจึงทำให้ถูกบุกรุก อ้างแบบนี้ไม่ได้เหมือนกับว่าเจ้าของบ้านไม่ได้ล็อกประตูบ้าน หากมีคนเข้ามาขโมยของก็จะอ้างว่าไม่ผิดเพราะเจ้าของบ้านไม่ล็อกประตูไม่ได้

ทำไมระบบเครือข่ายจึงถูกบุกรุกได้

ไม่มีระบบใดที่สามารถยืนยันความปลอดภัยได้ร้อยเปอร์เซ็นต์ ธนาคารที่มีระบบรักษาความปลอดภัยอย่างดี มีเจ้าหน้าที่รักษาความปลอดภัยเฝ้าตลอด 24 ชม. และมีเจ้าหน้าที่ตำรวจคอยตรวจตราก็ยังไม่สามารถยืนยันความปลอดภัยได้ แม้แต่สถานีตำรวจเองก็ยังมีข่าวว่าของหายหรือผู้ต้องหาหลบหนีได้ แล้วระบบเครือข่ายก็คงไม่สามารถยืนยันความปลอดภัยได้เช่นกัน เราคงเคยได้ยินข่าวว่าเว็บไซต์ของเอฟบีไอยังถูกบุกรุกอยู่บ่อย ๆ

สาเหตุที่ระบบเครือข่ายถูกบุกรุกก็เนื่องมาจากจะมีผู้ไม่หวังดีคอยค้นหารูรั่วหรือช่องโหว่ของระบบรักษาความปลอดภัยอยู่ตลอดเวลา และไม่ได้ทำเพียงคนเดียว แต่จะรวมกันทำเป็นกลุ่ม เมื่อค้นหารูรั่วหรือช่องโหวพบก็จะบอกต่อกันไปพร้อมกับบอกวิธีการบุกรุกระบบเครือข่ายโดยละเอียด ทำให้ผู้ใช้งานธรรมดาที่ได้รับทราบข้อมูลหล่านี้ก็สามารถบุกรุกระบบได้โดยที่ไม่ต้องค้นหาเองและไม่ต้องใช้ความรู้ความสามารถมากนัก

อีกอย่างเรามีค่านิยมที่ผิด ๆ ให้ความสำคัญกับแฮกเกอร์กันมากเกินไป คนที่ออกแบบและติดตั้งระบบเครือข่ายนั้นไม่ค่อยมีใครรู้จัก แต่คนที่เจาะระบบได้กับถูกให้ความสำคัญกว่า ลองคิดดูนะครับคนที่ออกแบบระบบเครือข่ายขององค์การนาซ่ากับคนที่เจาะระบบขององค์การนาซ่าได้ใครจะดังกว่ากัน... ค่านิยมเช่นนี้ทำให้การบุกรุกระบบเครือข่ายเพิ่มมาขึ้นทุกวัน

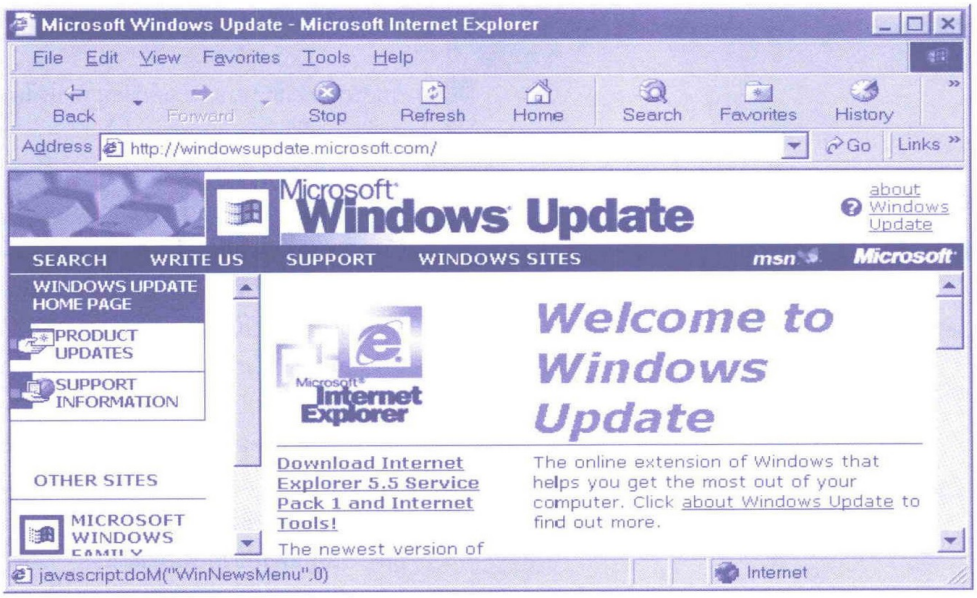
นับวันการบุกรุกเครือข่ายยิ่งง่ายขึ้น เนื่องจากประการแรกผู้ใช้งานทั่วไปมักจะมีความพยายามทำตัวเป็นแฮกเกอร์โดยจะค้นหาข่าวคราวว่ามีใครค้นพบรูรั่วบ้าง แล้วก็เอาข้อมูลเหล่านี้มาเจาะระบบผู้อื่น ประการที่สองผู้ดูแลระบบส่วนใหญ่มักเป็นมือใหม่และงานยุ่งไม่ค่อยมีเวลาตรวจสอบและติดตามข่าวคราวเกี่ยวกับวิธีการบุกรุกระบบ ทั้งสองสาเหตุนี้ก็เป็นเหตุสนับสนุนให้มีการบุกรุกระบบเครือข่ายเพิ่มมากขึ้น

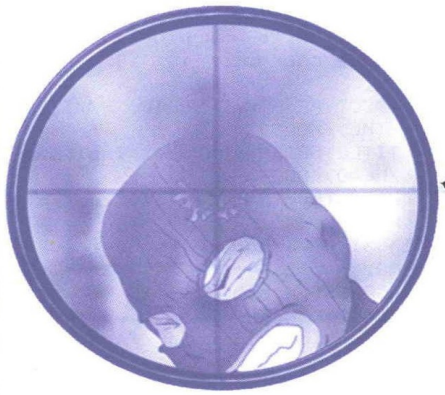
รูรั่วของระบบเครือข่ายไม่ยากที่จะตรวจพบและแก้ไข

ผู้ที่ทราบข้อมูลรอยรั่วของระบบเครือข่ายแล้วก็เปรียบเหมือนมีอาวุธอยู่ในมือที่สามารถนำไปใช้ทำอันตรายต่อผู้อื่นได้ และทำให้มีความรู้สึกว่าตนเองมีอำนาจทั้ง ๆ ที่ไม่ได้สร้างอาวุธนี้ขึ้นมาเอง เมื่อเป็นเช่นนี้เราจะต้องทำอย่างไรเพื่อไม่ให้เกิดเหตการณ์ลักษณะนี้

เมื่อมีผู้ไม่หวังดีที่คอยค้นหารูรั่วของระบบเครือข่ายอยู่ตลอดเวลา เราก็ต้องติดตามข่าวคราวเหล่านี้ตลอดเวลาเช่นกัน วิธีการที่ง่ายที่สุดก็คือการติดตามข้อมูลเหล่านี้จากระบบอินเทอร์เน็ตหรือเว็บไซต์ของแฮกเกอร์ต่าง ๆ และปรับปรุงระบบรักษาความปลอดภัยของเครือข่ายให้ทันกับรูรั่วต่าง ๆ ที่มีการค้นพบ

ในปัจจุบันรอยรั่วที่ถูกพบจะถูกแจ้งกลับไปยังเจ้าของผลิตภัณฑ์ เจ้าของผลิตภัณฑ์ก็จะทำการแก้ไขและอุดรอยรั่วอย่างรวดเร็วเราเพียงมีหน้าที่คอยตรวจสอบข้อมูลกับโฮมเพจของผลิตภัณฑ์ที่เราใช้ก็จะสามารถป้องกันรูรั่วได้ ตามปรกติการแก้ไขรูรั่วจะไม่กินเวลานานมากนัก ดังนั้นเมื่อมีการค้นพบรูรั่ว ถ้าเราไม่ใช่เครือข่ายที่สำคัญเป็นเป้าหมายของการโจมตีก็จะสามารถแก้ไขโดยการอุดรอยรั่วได้อย่างทันท่วงที





รูปที่ 8 แสดงโฮมเพจ Microsoft Update สำหรับดาวน์โหลดโปรแกรมเพื่ออุดรูรั่วของของผลิตภัณฑ์ไมโครซอฟท์

ตัวอย่างการอุดรูรั่วของบริษัทไมโครซอฟท์จะมีโฮมเพจให้เราสามารถดาวโหลดโปรแกรมเพื่ออุดรูรั่วของผลิตภัณฑ์ต่าง ๆ ได้ โดยให้เราเปิดโฮมเพจไปที่ Windows Update.microsoft.com ดังรูปที่ 8

สำหรับการแก้ไขรูรั่วของผลิตภัณฑ์อื่นก็มีวิธีการที่คล้ายคลึงกัน เราสามารถตรวจสอบได้จากโฮมเพจของเจ้าของผลิตภัณฑ์นั้นๆ หรือสอบถามจากตัวแทนจำหน่าย

ควรตรวจแก้ไขรูรั่วบ่อยแค่ไหน

ช่วงเวลาของการตรวจสอบรูรั่วนั้นยิ่งบ่อยยิ่งดี แต่ถ้าไม่มีเวลาอย่างน้อยก็คือควรตรวจสอบอย่างน้อยเดือนละครั้ง และมีวิธีที่ช่วยแบ่งเบาภาระในการตรวจสอบและแก้ไขรูรั่วดังนี้

- สมัครเป็นสมาชิกข่าว (mailing group) ของเว็บไซต์ต่างๆ ที่เกี่ยวกับการบุกรุกระบบเครือข่าย
- ติดตามข่าวคราวจากนิตยสารคอมพิวเตอร์ต่าง ๆ
- แจ้งให้ตัวแทนจำหน่ายผลิตภัณฑ์ส่งข้อมูลให้เราทันทีที่มีการเปลี่ยนแปลงข้อมูล
- เพิ่มการบริการบำรุงรักษาเครื่องและอุปกรณ์ต่าง ๆ ให้ทำการอุดรูรั่วของระบบด้วย
- ว่าจ้างบริษัทที่ปรึกษาให้ดำเนินการให้

ปรกติแฮกเกอร์ส่วนใหญ่จะเป็นแฮกเกอร์มือสมัครเล่นไม่ได้ทำเป็นอาชีพ ดังนั้นเราพอจะต่อกรด้วยไว้ ไม่ต้องกังวลจนเกินไปนักไม่ฉะนั้นระบบเครือข่ายของเราจะไม่ได้ใช้งานหรือใช้งานอย่างไม่เต็มที่

ใครเป็นคนผิดในเรื่องระบบรักษาความปลอดภัย

จากประสบการณ์การเป็นผู้ดูแลระบบของผู้เขียน เมื่อระบบถูกบุกรุกท่านผู้อ่านว่าใครเป็นคนผิด.... แน่นอนครับแฮกเกอร์ต้องเป็นคนผิด แต่ที่แน่นอนไปกว่านั้นแฮกเกอร์ไม่ได้ถูกตำหนิหรอกครับ เพราะไม่ทราบว่าตัวจริงที่แท้จริงของเขาคือใคร เขาจะตำหนิผู้ดูแลระบบมากกว่าเรียกว่าแทบตกงานเลยทีเดียว

"ดูแลระบบอย่างไรปล่อยให้แฮกเกอร์เข้ามาบุกรุกได้" เป็นคำพูดที่ทำร้ายจิตใจผู้ดูแลระบบมาก ทำไมเป็นอย่างนั้นละครับ ถ้าสมมุติว่ารถเราไม่ได้ติดสัญญาณกันขโมยแล้วถูกขโมยรถไป เจ้าของรถยังต้องถูกประนามเหมือนว่าเป็นคนผิดเองซะอย่างงั้น และการบุกรุกในบางกรณีผู้ใช้งานยังให้ความร่วมมือกับผู้บุกรุกด้วย และยิ่งผู้ดูแลระบบเข้มงวดต่อระบบรักษาความปลอดภัยมากเพียงไรผู้ใช้งานก็ใช้งานไม่สะดวกมากขึ้นเท่านั้น ดังควรจะเห็นใจซึ่งกันและกันและร่วมมือกันหาทางแก้ไขจะดีกว่า

ระบบรักษาความปลอดภัยสำหรับระบบเครือข่ายนี้เป็นงานที่ต้องอาศัยความร่วมมือและความเข้าใจจากทุกฝ่ายที่เกี่ยวข้อง และเป็นงานที่ต้องทำเพื่อป้องกันไม่ใช้งานที่ทำเพื่อแก้ไข ดังนั้นเราจึงต้องเริ่มทำก่อนที่จะเกิดเหตุการณ์บุกรุกระบบขึ้นและไม่ต้องกังวลมากจนไม่เป็นอันทำงานนะครับ ถ้าเราทำตามหน้าที่อย่างเต็มที่ด้วยความระมัดระวังแล้วยังเกิดความผิดพลาดอีกก็ไม่ถือว่าละเลยต่อหน้าที่